REMARKS/ARGUMENTS

1.) Claim Amendments

The Applicant has amended claims 10 and 11. Accordingly, claims 1-12 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Claim Rejections – 35 U.S.C. § 101

The Examiner rejected claims 10-11 under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. The Applicant has amended the claims to direct it toward statutory subject matter. The Examiner's consideration of the amended claims is respectfully requested.

3.) Claim Rejections – 35 U.S.C. § 103(a)

The Examiner rejected claims 1-5, 7-12 under 35 U.S.C. § 103(a) as being unpatentable over Graveman (US 6,851,052) and further in view of Lerner (US 6,718,503). The Applicant respectfully traverse the rejection. Regarding claims 1, 9, and 12, Graveman, which generally describes a method for generating an authentication code, has very few elements in common with claims 1, 9 or 12 and Lerner merely discloses an error correcting code. Further, there is no teaching, suggestion or motivation in either reference to combine these references.

The preamble of Claim 1 provides, in part, "A method of processing a message to determine a tag value from the message and from a key according to a message authentication code..." However, Graveman discloses a message and a key and, using these, the invention of Graveman is used to generate an Approximate Message Authentication Code which is transmitted together with the message. There is no correlation between the tag value of the present invention and the Approximate Message Authentication Code of Graveman.

Claim 1 further provides, in part: "selecting one of a plurality of symbols..." Even if the vectors of Graveman are comparable to the symbols of the present invention

(which they are not since the vectors of Graveman do not constitute a codeword of an error correcting code), it is not possible to map this element to Graveman, because Graveman does not choose one of the vectors.

Claim 1 further provides, in part: "the plurality of symbols forming a codeword encoding a data item derived from the message..." The Examiner does not indicate which element(s) of Graveman correlate to the codeword and the data item nor how the vectors encode the data item.

Claim 1 further provides, in part: "the codeword encoding the data item according to an error correcting code..." Graveman does not use an error correcting code, so the Examiner relies on Lerner. It is noted that there are hundreds, if not thousands, of error-correcting codes. Different aspects and encoding methods have been extensively studied in academia and industry. Lerner is one very narrow application of an error correcting code—that is an interleaving method of error correcting code words to avoid burst error problems when transmitting over power line carrier systems.

There is nothing in Lerner to teach, suggest or motivate a combination with Graveman as Graveman is not based on error correcting code techniques and, in particular, is not directed or suggestive of interleaved error correcting code techniques.

A key feature of the present invention is to apply an error correcting code to the authentication process: "said key determines which one of said plurality of symbols is selected..." Because, as noted above, there is no selection in Graveman, this element cannot be mapped to Graveman. In Graveman, a key is used to permute the message.

Claim 1 finally provides, in part: "determining the tag value to be the selected symbol." As noted above, there is no tag value and no selected symbol in Graveman.

As noted, Graveman, which generally describes a method for generating an authentication code, has very few elements in common with claims 1, 9 or 12 and Lerner merely discloses an error correcting code. Further, there is no teaching, suggestion or motivation in either reference to combine these references. Even if the references were combined, one would not arrive at the claimed invention. For example, there would not be an element of determining a tag value. Furthermore, a method based on the cited references would not comprise "selecting one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from

the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and determining the tag value to be the selected symbol".

Graveman discloses so-called "approximated message authentication codes" (AMAC) using the following encoding method: (1) Arrange the message bits in a matrix with A columns and T^2 rows; (2) Permute the message bits using a suitable secret key dependent pseudo-random function; (3) Encrypt the permuted message bits using a secret key; (4) Apply a bit majority function on T rows at the time this result in a new A time T matrix; (5) Apply the very same (as in step 4) majority function on the A times T matrix. This results in the AMAC function according to Graveman. The foregoing is inapposite the present invention because:

(1) The present invention claims a method based on code words from an "error correcting code." The Graveman matrix arrangement has nothing to do with error correcting codes and the method cannot be used together with an error correcting code as such a code does not have the properties Graveman needs in order to construct a secure AMAC according to that method.

(2) The present invention claims a method wherein the message authentication code is based on selecting "one of a plurality of code symbols" while Graveman teaches a method that is based on taking a majority function on different specific chosen sets of bits of the original permuted and encrypted message.

(3) Graveman teaches a method where the secret key is used to *permute* the plain text message bits and then encrypt the permuted message prior to applying a majority function on the resulting new message. This is a very different usage of the key compared to using the key to determine which of a plurality of code symbols to use for the encoding the message. In particular, *no encryption step* at all is performed in the method claimed in the present invention.

Claims 2-5 and 7-8 depend from claim 1 and recite further limitations in combination with the novel elements of claim 1. Therefore, the allowance of claims 1-5 and 7-12 is respectfully requested.

The Examiner rejected claims 5-6 under 35 U.S.C. § 103(a) as being unpatentable over Graveman in view of Lerner, and further in view of Shokrollahi (US 6,631,172). As noted above, Graveman fails to disclose all of the elements of independent claim 1 and Lerner and Shokrollahi remedy the deficiency.

Claims 5 and 6 depend from claim 1 and recite further limitations in combination with the novel elements of claim 1. Therefore, the allowance of claims 5 and 6 is respectfully requested.

4.) Prior Art Not Relied Upon

In paragraph 8 of the Office Action, the Examiner stated that the prior art made of record and not relied upon is considered pertinent to the Applicant's disclosure. None of the cited art alone disclose, or together, teach or suggest the present invention as claimed in claims 1-12.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

/Michael Cameron, #50,298/

Date: June 5, 2007

Michael Cameron
Registration No. 50,298

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024
(972) 583-4145
michael.cameron@ericsson.com